ISSN 0974 - 9373

Vol. 27 No. 1 (2023) **J. Int. Acad. Phys. Sci.** pp. 1-12

Generalized MacWilliams Identities on SKE Weights for Linear Codes over Ring Z_q

Meenakshi Sridhar
Department of Computer Science, Rajdhani College,
Univesity of Delhi, New Delhi, India
Email : meenakshi.sridhar.sharma@gmail.com

Manohar Lal (Kaushik)
School of Computer & Inf. Sciences, New Delhi-110068, India
Email : prof.manohar.lal@gmail.com

(Received January 23, 2023, Accepted February 25, 2023)

Abstract: In Coding Theory/ Error-Correcting codes, the concept of *distance*, or of *metric*, is used as a measure of degree of dissimilarity between two words of equal length, which may be transmitted/ received in communication systems, or stored/ retrieved in digital storage devices. For the *Euclidean-type*, one of the types of distances, distance (or sometime, the square of the distance) between two words $a = (a_0, a_1, \ldots, a_n)$ and $b = (b_0, b_1, \ldots, b_n)$ is the sum of the *squares* of the values—under the particular metric/distance of Euclidean-*type*—of differences $(a_i - b_i)$ in the corresponding tuples of the two words a and b, for $i = 1, 2, \ldots, n$. Euclidean-type distance is (*i*) regarded as the most relevant measure of efficiency for symmetric PSK-codes, (*ii*) used in wireless LAN standard IEEE 802.11b-1999, and (*iii*) extensively applied in analysis of convolution codes and Trellis codes.

On the other hand, MacWilliams Identities provide a mechanism for deriving properties of large codes from corresponding properties of (generally very) small codes. The identities, which relate weight-enumerators of a code and its dual code, were first derived in 1963 by MacWilliams[1] for linear codes over finite fields for Hamming metric. MacWilliams-type identities for *Sharma-Kaushik metrics* (*SK-metrics*) are discussed[2].

In this paper, we investigate the more general case of the possible MacWilliams-type identities for *Sharma-Kaushik Euclidean distance* (*SKE distance*), a *new concept* to be defined. These investigations generalize the MacWilliams identities for Euclidean distance discussed in[2-3]. The results in the investigation have the potential for improving (*i*) the wireless LAN standard IEEE 802.11b-1999 (*ii*) functioning of MANET, VANET & other networks.

Keywords: Error-correcting Code, MacWilliams identity, Euclidean weight enumerator, Sharma-Kaushik Euclidean weight (SKE weight, wt_SKE), Sharma-Kaushik Euclidean metric (SKE-metric), Sharma-Kaushik Euclidean weight enumerator (SKE weight enumerator).

1. Introduction

In the field of Coding Theory, including the Theory of Error Correcting Codes, the concept of *distance*, or of *metric*, is used as a measure of degree of dissimilarity between two words of equal length, which may be transmitted/ received in digital communication systems, or stored/ retrieved in digital storage devices. For digital systems, the concept was introduced and first used, between 1947 and 1950, by three pioneers of field: Richard W. Hamming, C. E. Shannon, & M J E Golay[4-6]. Hamming, probably, is the first to conceive the concept[5], hence the first metric for digital systems is called *Hamming metric*.

At the outset, it may be pointed out that the concepts of 'distance' and 'weight' are quite closely related, and may be interchangeably used, particularly for codes, over rings & fields, because, for a metric d and corresponding weight w, we have the relation $d(x,0) = w(x)$.

Out of the various ways in which the *concept of distance* for digital systems is characterized, the *Hamming-type* distances and the *Euclidean-type* distances are well-known. The Hamming metric, Lee metric, and Sharma-Kaushik metric are well-known examples of *Hamming-type distances***,** in which the distance between two words $a = (a_0, a_1, \ldots, a_n)$ and $b = (b_0, b_1, \ldots, b_n)$ is the *sum of the values*—under the particular metric/distance of Hamming-*type*—of differences $(a_i - b_i)$ in the corresponding tuples, for $i = 1, 2, \ldots, n$. Hamming-type distances have been extensively studied and used.

On the other hand, for the *Euclidean-type distances*, the distance (or sometime, the square of the distance) between two words $a = (a_0, a_1, \ldots, a_n)$ and $b = (b_0, b_1, \ldots, b_n)$ is the *sum of the squares of the values*—under the particular metric/distance of Euclidean-*type*—of the differences $(a_i - b_i)$ in the corresponding tuples, for $i = 1, 2, \ldots, n$.

Euclidean-type distance is regarded as the most relevant measure of efficiency for symmetric PSK-codes, because correction to the closest codeword in squared Euclidean distance is the same as maximum likelihood decoding (MLD) w.r.t. Additive white Gaussian noise (AWGN) channel[7]. The wireless LAN standard IEEE 802.11b-1999 uses a variety of different Euclidean-type PSK's depending on the data rate required. Also, Euclidean distance is extensively applied in the analysis of convolution codes and Trellis codes, whereas Hamming distance is frequently encountered in the analysis of block codes.

Two well-known *Euclidean-type* distances are *Euclidean-Lee* distance (generally called as *Euclidean distance* only, without the suffix *Lee*), and *Euclidean-PSK*.

Apart from the 'Conclusion' section, the paper has *five* sections including this 'Introduction'. *Section 2* discusses various basic concepts and significance of each. *Section 3* discusses a mechanism, called *Gray map*, which for a given metric, say M, converts each m-tuple, say X, with weight(X), under the given metric M, over a ring Z_q to some tuple Y, of length n—which is some fixed multiple of m over Z_q, such that $\text{weight}_M(X) = \text{weight}_H(Y)$, where $\text{weight}_H(Y)$ denotes Hamming weight of Y. This mechanism is used in deriving MacWilliams-type identities for linear codes with a given metric from the already established corresponding identities for linear codes with Hamming metric. In *Section 4*, the core of this paper, we establish the MacWilliams-type identities for linear codes with SKE distances. *Section 5* discusses *potential applications* of the established results. In the rest of this section, we briefly discuss the significance, in the area of error-correcting codes, of the two major terms in the title, viz. *MacWilliams's identities* and *SKE weight*.

MacWilliams Identities, irrespective of the distance used, provide a mechanism for deriving properties of large codes from the corresponding properties of (generally very) small codes. The identities involve the concept of *weight-enumerator*, which is significant in view of the fact that it contains significant information about a code, including its minimum distance, and the probabilities of decoding error and failure etc[8]. The identities were first derived in 1963 by MacWilliams[1] for linear codes for Hamming metric. These identities for Lee distance, a Hamming-*type* distance, and for (Lee-) Euclidean distance, are discussed[3]. Also, MacWilliams-type identities for *Sharma-Kaushik metrics (SK-metrics)*, which are *Hamming-type* metrics, are discussed[2].

Significance of Sharma-Kaushik metrics & SKE weights: The SKE-metrics are important in coding theory because these can provide appropriate measures for various possible modulation schemes. Additionally, the corresponding SKE enumerators give much more information than the Hamming enumerator, while requiring, in some cases, even less than half as many variables as the complete enumerator[9].

2. Basic Concepts

In this section we briefly discuss the following concepts, along with significance of each Dual Code, Sharma-Kaushik metric, Euclidean weight, Euclidean weight enumerator, Sharma-Kaushik Euclidean weight (SKE

weight), Sharma-Kaushik Euclidean weight enumerator (SKE weight enumerator).

2.1. Dual Code. MacWilliam identities relate the weights of a code C and weights of its dual code $C^{\perp}$. For a linear code C of length n over the ring Z_q, its dual code, denoted by $C^{\perp}$, is given by

$$C^{\perp} = \{(c_1, c_2, \ldots, c_n) \in (Z_q)^n : \sum_{i=1}^{n} c_i \cdot d_i = 0, \forall\ (d_1, d_2, \ldots, d_n) \in C\}.$$

2.2. Sharma-Kaushik metrics & weight-functions[10-15]

For integers q > 1, and $m \geq 1$, consider a partition $\mathcal{P}$ of $Z_q = \{0, 1, \ldots, (q-1)\}$ into (disjoint, nonempty) subsets $B_0, B_1, \ldots, B_{m-1}, B_m$, such that

i. $B_0 = \{0\}$

ii. For $i \in Z_q$, $i \in B_s \Leftrightarrow (q - i) \in B_s$

iii. If $i \in B_s$, *and* $j \in B_t$, and $s > t$ (as Natural numbers) then

$$\min\{i, q-i\} > \min\{j, q-j\}$$

iv. If $s > t$, then $|B_s| \geq |B_t|$, except for $s = m$, in which case we may have

$$|B_m| \geq (1/2)\,|B_{m-1}|,$$

where $|B|$= number of elements in the set B.

The partition $\mathcal{P}$ now known as *Sharma-Kaushik partition, or SK-partition* introduces a weight-function

(1) $wt\_SK_{\mathcal{P}}: Z_q \rightarrow \{0, 1, \ldots, m\}$, s.t if $i \in B_s$, then $wt\_SK_{\mathcal{P}}(i) = s$.

From the definition above, for $i \in Z_q$,

(2) $$max.\ (wt\_SK(i)) = m.$$

Further, for a codeword $c = (c_1, c_2, \ldots, c_n)$, with $c_i \in Z_q$,

(3) $$wt\_SK_{\mathcal{P}}(c) = \sum_{i=1}^{n} wt\_SK(c_i)$$

The weight-function $wt\_SK_{\mathcal{P}}$ is now known as *Sharma-Kaushik weight-function corresponding to the partition* $\mathcal{P}$.

For two code words $c = (c_1, c_2, \ldots, c_n)$ and $c' = (c'_1, c'_2, \ldots, c'_n)$ of C, the weight-function wt_SK defines a *metric*, called *Sharma-Kaushik metric, or SK-metric*, between two code-words of code C as follows

$$d_{SK\text{-}\mathcal{P}}(c, c') = wt\_SK_{\mathcal{P}}(c - c'), \text{ where}$$

$$c - c' = (c_1 - c_1', c_2 - c_2', \ldots, c_n - c_n').$$

The discussion above gives rise to a method of generating metrics, and not just a method of defining a particular metric or weight function. For each partition $\mathcal{P}$, there exists one weight function $wt\_Sk_{\mathcal{P}}$ and one SK-metric

$d_{SK\text{-}\mathcal{P}}$. Thus, there are possibly a number of weight functions and SK-metrics. For the rest of the discussion, it is assumed that partition $\mathcal{P}$ is fixed and the suffix $\mathcal{P}$ is dropped, and only the notations *wt_Sk* and d_{SK} are used.

As mentioned earlier, the idea of SK-partition, leads not merely to a single weight/ metric, but proposes a scheme of generating different weights and metrics for error-correcting codes. According to the scheme, Z_q may be partitioned in a number of ways, with each partition leading to a different weight/ metric. Specific partitions lead to some well-known weights / metrics. For example, the partition

$$\mathcal{P}_H = \{B_0 = \{0\}, B_1 = \{1, 2, \ldots, (q-1)\}\}$$

yields the Hamming-weight function *wt_H*, and the partition

$$\mathcal{P}_L = \{B_0 = \{0\}, B_i = \{i, (q-i)\}: 1 \leq i \leq \lfloor q/2 \rfloor, \text{the integral part of } q/2\}$$

yields Lee-weight function *wt_L*.

Thus, the Hamming metric d_H and the Lee metric d_L become special cases of d_{SK}. The weight enumerator contains information about a code, including its minimum distance, the number of Code words of each weight, and the probabilities of decoding errors and failures[8].

MacWilliams identities for (Lee-)*Euclidean* weights are proved[3]. One of the objectives of this paper is to prove the identities to more generalized case of SKE weights. In subsection 2.3, we introduce the concepts of *Euclidean weight & Euclidean weight enumerator*, and in subsection 2.4, we discuss the concepts of SKE weight and SKE weight enumerator.

2.3. Euclidean weight & Euclidean weight enumerator

For a code C, of length n, over a ring Z_q, the Lee-weight *wt_L* is given by

wt_L (0) =0; and for $1 \leq i \leq \lfloor q/2 \rfloor$, we have

(4) $$wt\_L(i) = i, \text{ and } wt\_L(q-i) = i.$$

The maximum value of $\{wt\_L(i): i = 0, 1, 2, \ldots, (q-1)\} = \lfloor q/2 \rfloor$.

(5) $$\text{Let } Cmax = (\lfloor q/2 \rfloor)^2$$

The *Euclidean weight* of an *n*-tuple $c = (c_1, c_2, \ldots, c_n)$ over ring Z_q is defined as[3]

(6) $$wt\_E(c) = \sum_{i=1}^{n} (wt\_L(c_i))^2.$$

The corresponding Euclidean-weight Enumerator of a linear code C of length n over Zq is defined as

$$EW_C(x, y) = \sum_{i=0}^{n \times Cmax} A_i \, x^{n \times Cmax - i} \, y^i,$$

where A_i is the number of code-words of Euclidean-weight of *i*.

2.4. SKE weight & SKE weight enumerator

SKE weight: Recalling from subsection 2.2, a partition $\mathcal{P}$ of Z_q = {0, 1, …, (q –1)} into (disjoint, nonempty) subsets B_0, B_1, …, B_{m-1}, B_m, introduces a weight-function
$wt\_SK_{\mathcal{P}}$: $Z_q \rightarrow$ {0, 1, …, m}, s.t

if $i \in B_s$, then $wt\_SK_{\mathcal{P}}(i) = s$.

From the definition above, for i$\in Z_q$, *max.* $(wt\_SK(i)) = m$.
Then, the *Sharma-Kaushik Euclidean weight (SKE weight)* of a codeword $c = (c_1, c_2, \ldots, c_n)$, with $c_i \in Z_q$ is given by

(8) $$wt\_SKE_{\mathcal{P}}(c) = \sum_{i=1}^{n} (wt\_SK(c_i))^2$$

The corresponding SK-Euclidean-weight Enumerator (SKE weight enumerator) of a linear code C of length n over Zq is defined as

(9) $$SKEW_C(x, y) = \sum_{i=0}^{n \times m \times m} A_i \, x^{n \times m \times m - i} \cdot y^i,$$

where A_i is the number of code-words of SKE weight of *i*.

3. Weight-preserving map from SKE code to Hamming code

The use of Gray map (to be defined below) in the landmark paper[16] where it was shown that interesting binary codes could be found as images of linear codes having some other underlying metric led to the Gray map becoming a useful tool for deriving weight-related properties of codes over rings Z_q with some non-Hamming metric from the already established properties of binary codes (with Hamming metric).

The Gray map converts each m-tuple, say X with $weight_M(X)$, under a given (non-Hamming metric) M, over a ring Z_q to some tuple Y, of length n which is some fixed multiple of m over Z_q, such that $weight_M(X) = weight_H(Y)$, where $weight_H(Y)$ denotes Hamming weight of Y. The Gray map preserves weight-related properties of the codes. This mechanism is used in deriving those weight-related property of a code, including MacWilliams-type identities for linear codes, which are already established for binary codes.
Here, we use Gray map to establish MacWilliams identities for codes with SKE weight. The required Gray map is defined as follows.
For a fixed integer q >1, let the SKE-weight function, *wt_SKE* correspond to the partition

$$\mathcal{P} = \{B_0, B_1, B_2, \ldots, B_{m-1}, B_m\} \text{ of } Z_q,$$

Further, let t $\geq$ *Max. {|Bi|: i =0, …, m}, and t be any divisor of q and a prime power, and* F_t *be a finite field with t elements.*

It may be noted that under SK-metric, corresponding to the above partition, the maximum weight $\{i: i \in Z_q\} = m$. Hence,

(10) $\quad$ Max. wt_SKE $\{i: i \in Z_q\} = m^2$.

[1]Define the function $\theta: Z_q \rightarrow (F_t)^{m\times m}$,
for $x, y \in Z_q$; and $0 \neq a_k \in F_t, 0 \neq b_k \in F_t$,
as follows

Case I: if wt_SKE(x) = $i < m^2$; and $0 < x < \lfloor q/2 \rfloor$, then
$\theta(x) = (0, ..., 0, a_{m\times m-i+1}, ..., a_{m\times m})$.
Further, if y is such that $y \neq x$, $0 < y < \lfloor q/2 \rfloor$ with wt_SKE(y) = $i < m$, then
$\theta(y) = (0, ..., 0, b_{m\times m-i+1}, ..., b_{m\times m})$, with $0 \neq b_k \neq a_k \neq 0$ for at least one k.

Case II: if wt_SKE(x) = $i < m^2$ and $\lfloor q/2 \rfloor < x < q$, then
$\theta(x) = (a_1, ..., a_i, 0, ..., 0)$,
Further, if y is such that $y \neq x$, $\lfloor q/2 \rfloor < y < q$ with wt_SKE(y) = $i < m^2$, then
$\theta(y) = (b_1, \ldots, b_i, 0, \ldots, 0)$, with $0 \neq b_k \neq a_k \neq 0$ for at least one k.

Case III: if wt_SKE(x) = m^2, then
$\theta(x) = (a_1, ..., a_i, \ldots, a_{m\times m})$
and for $y \neq x$ and wt_SKE(y) = m^2
$\theta(y) = (b_1, ..., b_i, \ldots, b_{m\times m})$, with $0 \neq b_k \neq a_k \neq 0$ for at least one k.

Choice for such a $b_k (\neq 0) \in F_t$ in each of the three cases is possible, as $t \geq$ Max. $\{|B_i| \text{ for } i = 1, 2, \ldots, m\times m\}$.

As, for $x \neq y$, $\theta(x) \neq \theta(y)$, therefore $\theta: Z_q \rightarrow (F_t)^{m\times m}$ is an injection, but not necessarily bijection, for which the condition $q = t^{m\times m}$ should necessarily be satisfied, because for θ to be bijection $q = |Z_q| = |(F_t)^{m\times m}| = t^{m\times m}$.

Theorem 3.1. *For any ring Z_q ($q \geq 2$), and with the notations t and m etc. as discussed above, there exists a Gray map (say) ϕ from $(Z_q)^n$ to $((F_t)^{m\times m})^n$ and the map ϕ is a weight preserving injective map from $((Z_q)^n$, wt_SKE) to $(((F_t)^{m\times m})^n$, wt_H), where wt_H denotes Hamming weight of n-tuple over $(F_t)^{m\times m}$. Further, for a code C of length n over Z_q with wt_SKE as weight function*

(i) $\quad |C| = |\phi(C)|$, *and*

---

[1] For the proposed function $\theta: Z_q \rightarrow (F_t)^{m\times m}$, the number t is chosen taking into consideration the following two criteria:

(i) F_t should be a field; therefore, t should be a prime power

(ii) elements of Z_q having same weight, should be representable distinctly by (distinct) elements of F_t. Hence,

$t \geq$ Max. $\{|Bi|: i = 0, \ldots, m\}$

The number m^2 in $(F_t)^{m\times m}$ is used in view of the fact that each element x of Z_q—with *SKE-w* as its weight under SKE-metric—is to be mapped to some m-tuple $(x_1, x_2, \ldots, x_{m\times m})$ having SKE-wt non-zero elements of F_t, or equivalently having SK-w Hamming weight, with $m\times m$ being the maximum under each of wt_SKE and Hamming weight.

(ii) *ϕ (C) is the corresponding code with wt_H weight, and the corresponding weight enumerators are related by* $SKE_C(x, y) = H_{\phi(C)}(x, y)$.

Proof: The map $\theta: Z_q \rightarrow (F_t)^{m\times m}$, defined just above, can be extended to a map, through *component-wise mapping*, to the map

$$\phi: (Z_q)^n \rightarrow (F_t)^{m\times m})^n, \text{ for a natural number } n>1,$$

such that for $x = (x_1, x_2, \ldots, x_n), \in (Zq)^n$ with $x_i \in Z_q$,

$$\phi(x) = (\theta(x_1), \theta(x_2), \ldots, \theta(x_n))$$

The map ϕ being defined component-wise from the map $\theta: Z_q \rightarrow (F_t)^{m\times m}$, where θ is an injection—is also an injection.

More explicitly, we have proved that there exist an injective map ϕ, which maps $x = (x_1, x_2, \ldots, x_n), \in Z_q^n$ with $wt\_SKE(x) = \sum_1^n wt\_SKE(x_i) = W_x$ (say) to $\phi(x) = (\theta(x_1), \theta(x_2), \ldots, \theta(x_n)) \in ((F_t)^{m\times m})^n$, having $wt\_H(\phi(x))$ equal to W_x, implying that the map $\phi: ((Z_q)^n, wt\_SKE) \rightarrow ((F_t)^{m\times m})^n, wt\_H)$, *is weight preserving*.

Hence, from the fact that ϕ is injective, for any code C of length n over Z_q,

$$|C| = |\phi(C)|.$$

Also, by the fact that ϕ is weight preserving, $SKE_C(x, y) = H_{\phi(C)}(x, y)$.

In the rest of the discussion, even θ may be denoted by ϕ, unless the distinction is essentially required.

Next, we discuss the MacWilliams type identity on SKE-weight enumerator.

4. A MacWilliams type identity on SKE-weight enumerator for linear codes over Z_q

We start the discussion on MacWilliams type identity on SKE-weight enumerator with the following

Theorem 4.1. *Let* C *be a linear code of length* n *over* Z_q, *and the notations be as before. Then there exists a code C' of length* $m^2.n$ *over* F_t *satisfying*

$$H_{C'}(x, y) = (1/|\phi(C)|) H_{\phi(C)}(x + (t-1).y, x - y),$$

where $H_\$(x,y)$ *denotes Hamming-weight enumerator of the code \$. For the linear code* C, *the codes* ϕ(C), *and* C' *may not be linear, yet each has only one codeword of weight zero viz*. (0, 0, …, 0).

Proof: For the *linear* code C of length n over Z_q, let t (>1) be a positive divisor of q and a prime power. Further, let the map ϕ be a weight preserving map from $((Z_q)^n, wt\_SKE)$ to $((F_t)^{m\times m})^n, wt\_H)$. Such a map exists by the Theorem 3.1. Then ϕ(C) is a code of length $m^2.n$ over F_t, which is *not* necessarily linear. Let $H_{\phi(C)}(x, y)$ be the Hamming weight enumerator of the

code ϕ(C). However, MacWilliams Identities are true even for non-linear codes [17], and hence for ϕ(C) also. Of course, in this case, the MacWilliams identity does not involve the dual code $C^{\perp}$, but some other code, say, C'.
Thus, MacWilliams transform $H_{C'}(x, y)$ of $H_{\phi(C)}(x, y)$—where $H_{C'}(x, y)$ corresponds to a code C' of length $m^2.n$ over F_t—has the relation

$$H_{C'}(x, y) = (1/|\phi(C)|)\, H_{\phi(C)}(x + (t-1)\, y, x - y)$$

This proves the first part of the Lemma.
Also, as ϕ(C) is not necessarily linear, hence, C' is *not* necessarily the dual code $C^{\perp}$ *of C.* However, *if* ϕ(C) is a linear code, *then*[17] $C' = \phi(C)^{\perp}$.
Next, we prove remaining part: codes ϕ(C), and C' each has *only one* codeword of weight zero.
To show ϕ(C) has only one codeword of weight zero: As *C* is assumed to be a *linear* code of length n over Z_q, hence, the number of code words in *C* of wt_SKE (0) is 1. By definition, the map ϕ is weight preserving mapping, Therefore, in the code *ϕ*(*C*), number of code words of Hamming weight 0 is 1.
T*o show C' has only one codeword of weight zero:*
For the Hamming-weight enumerator $H_{C'}(x, y)$, let $H_{C'}(x, y) = \sum_{j=0}^{mn} A'_j\, x^{n-j} y^j$, then for x=1 and y=0, we get

$$H_{C'}(1, 1) = A'_0$$

But by first part of the lemma,

$$H_{C'}(x, y) = (1/|\phi(C)|)\, H_{\phi(C)}(x + (t-1).\, y, x - y)$$

Thus, for x=1 and y=0, we get

$$A'_0 = (1/|\phi(C)|)\, H_{\phi(C)}(1,1)$$

Further, let $H_{\phi(C)}(x, y) = \sum_{j=0}^{mn} B'_j\, x^{n-j} y^j$, then

$$H_{\phi(C)}(1,1) = \sum_{j=0}^{n} B'_j = \text{number of code words in } \phi(C) = |\phi(C)|.$$

$A'_0 = (1/|\phi(C)|)\, H_{\phi(C)}(1,1) = (1/|\phi(C)|)\, |\phi(C)| = 1.$
Next, we discuss the main result.

Theorem 4.2. *Let* C *be a linear code of length* n *over* Z_q, *and let* t (>1) *be a positive divisor of* q *and a prime power. Then the linear code* C *has a MacWilliams type identity on the wt_SKE over* Z_q *with the form*

(11) $$SKE_{C^{\perp}}(x, y) = (1/|C|)\, SKE_C(x + (t-1).\, y, x - y)$$

if and only if the following conditions are satisfied

1. *there exists a bijective map ϕ from* $(Z_q)^n$ *to* $(F_t)^{m\times m})^n$ *and the map ϕ is a weight preserving map from* $((Z_q)^n$, *wt_SKE) to* $((F_t)^m)^n$, *wt_H);*
2. *there exists a code C' of length* $m^2.n$ *over* F_t *and the MacWilliams transform* $H_{C'}(x, y)$ *of* $H_{\phi(C)}(x, y)$ *satisfies* $H_{\phi(C^{\perp})}(x, y) = H_{C'}(x, y)$.

Proof: The following proof is exactly on the lines of the proof for corresponding Theorem 4.2 of the paper[3] for MacWilliams Identities on the Lee weights.

First, suppose that the linear code C satisfies MacWilliams type identity (11)

By Theorem 3.1, for the code C of length n over Z_q and with wt_SKE, there is a one-to-one map ϕ so that code $\phi(C)$ is a code of length $m^2.n$ over F_t and the corresponding weight-enumerators satisfy

(12) $$SKE_C(x, y) = H_{\phi(C)}(x, y).$$

In eq. (12), $\phi(C)$ is a Hamming-weight code of length $m^2.n$ over F_t, whether linear or not. However, even a nonlinear code satisfies MacWilliams-type identities [17]. Thus, for the Hamming-weight code $\phi(C)$, there exists a code C' of length m^2. n over F_t satisfying the equality

(13) $$H_{C'}(x, y) = (1/|\phi(C)|) H_{\phi(C)}(x + (t-1)y, x - y).$$

Similarly, for the code $C^{\perp}$, by Theorem 3.1

(14) $$H_{\phi(C^{\perp})}(x, y) = SKE_{C^{\perp}}(x, y).$$

Also, in the statement of the theorem, it is assumed that

$$SKE_{C^{\perp}}(x, y) = (1/|C|)\, SKE_C(x + (t-1).\, y, x - y)$$

But by Theorem 3.1

(15) $$SKE_C(x + (t-1).\, y, x - y) = H_{\phi(C)}(x + (t-1)y, x - y)$$

From (14), (11), and (15), we get

(16) $$H_{\phi(C^{\perp})}(x, y) = (1/|C|) H_{\phi(C)}(x + (t-1)y, x - y)$$

From (13) and (16)

(17) $$|\phi(C)|\, H_{C'}(x, y) = |C|\, H_{\phi(C^{\perp})}(x, y),$$

If $H_{c'}(x, y) = \sum_{i=0}^{m\times m\times n} A_i\, x^{m\times m\times n-i}.\, y^i$; $H_{\phi(C^{\perp})}(x, y) = \sum_{i=0}^{m\times m\times n} A'_i\, x^{m\times m\times n-i}.\, y^i$.

By comparing the coefficients of $x^{m\times m\times n}$, obtained by taking i=0, we obtain

$$|\phi(C)|\, A_0 = |C|\, A'_0$$

But by the above theorem, and the fact that if C is linear, then the code $C^{\perp}$ is also linear, $A_0 = A'_0 = 1$, each being number of code-words of weight 0, giving

$$|C| = |\phi(C)|,$$

and hence, by (17),

$$H_{\phi(C^{\perp})}(x, y) = H_{C'}(x, y).$$

Conversely, let conditions 1. and 2. of the theorem be true and to establish (11)

By condition 1. there exists a bijective map ϕ from $(Z_q)^n$ to $((F_t)^{m\times m})^n$ and the map ϕ is a weight preserving map from $((Z_q)^n$, wt_SKE) to $((Ft)^{m\times m})^n$, wt_H). As ϕ is a bijective map, $|C| = |\phi(C)|$

Furthermore, for the Hamming-weight code $\phi(C)$, there exists a code C' of length $m^2.n$ over F_t and the MacWilliams transform $H_{C'}(x, y)$ of $H_{\phi(C)}(x, y)$satisfying

$$H_{C'}(x, y) = (1/|\phi(C)|)\, H_{\phi(C)}(x + (t-1).\, y, x - y).$$

Using condition 2. in the statement of the theorem, viz,

$$H_{C'}(x, y) = H_{\phi(C^{\perp})}(x, y), \text{ we get}$$

$$H_{\phi(C^{\perp})}(x, y) = (1/|\phi(C)|)\, H_{\phi(C)}(x + (t-1)y, x - y).$$

Using condition 1. in the statement of the theorem, for each of the two sides of the above equality, we get

$$SKE_{C^{\perp}}(x, y) = (1/|\phi(C)|\, SKE_C(x + (t-1)\, y, x - y)$$

Using $|C| = |\phi(C)|$, we get

$$SKE_{C^{\perp}}(x, y) = (1/|C|)\, SKE_C(x + (t-1).\, y, x - y).$$

Thus, from the theorem we get a necessary and sufficient condition for the existence of a MacWilliams type identity on the SKE-weight enumerator for linear codes over Z_q.

5. Potential Applications

The results in the investigation have the potential for (*i*) discovering properties of the symmetric PSK codes with very large number of code words *through* corresponding properties for the symmetric PSK-codes with (generally very) small number of code words for various metrics, (*ii*) improving the wireless LAN standard IEEE 802.11b-1999 (*iii*) improving functioning of MANET, VANET & other networks.

4. Conclusion

We have extended MacWilliams identities—already established for Linear codes for (*i*) Hamming metrics[1], (*ii*) Lee metrics[3], and (*iii*) SK-metrics[2] to the case of Sharma-Kaushik-Euclidean metric (SKE-metric). Apart from theoretical significance of the results, these have potential for applications for improving the functioning of (*i*) the wireless LAN standard IEEE 802.11b-1999, and (*ii*) MANET, VANET & other networks.

Dedication: This research article is dedicated to the profound memory of (Late) Prof. P.N. Pandey, the founder General secretary of IAPS, who actually inspired us for active academic activities including writing of this paper.

References

1. F. J. MacWilliams; A theorem on the distribution of weights in a systematic code, *Bell System Technical Journal* (1963).
2. Meenakshi Sridhar, Manohar Lal Kaushik; MacWilliams type identities on Sharma-Kaushik weights for linear codes over ring Zq (communicated)
3. Tang Yongsheng, Zhu Shixin, Kai Xiaoshan; MacWilliams type identities on the Lee and Euclidean weights for linear codes over Z_{ℓ}, *Linear Algebra and its Applications* 516 (2017), 82-92.
4. Richard W Hamming; Error detecting and error correcting codes, *The Bell system technical journal* 29(2) (1950), 147-160.
5. Claude Elwood Shannon; A mathematical theory of communication, *The Bell system technical journal* 27(3) (1948), 379-423.
6. Marcel JE. Golay, Notes on digital coding, *Proc. IEEE* 37 (1949), 657.
7. Viswanathan Mathuranathan; *Wireless Communication Systems in MATLAB-Gaussian Waves* (second edition), 2020.
8. E.R. Berlekamp; *Algebraic Coding Theory*, World Scientific Publishing Co. Pvt. Ltd., 1984.
9. E. R. Berlekamp; *Algebraic Coding Theory*, World Scientific, 2015.
10. Manohar Lal Kaushik; Burst-Error-Correcting Codes with Weight constraints under a New Metric, *Journal of Cybernetics*, 8 (1978), 183-202.
11. B. D. Sharma and Manohar Lal Kaushik; Limited Intensity Random and Burst Error Correcting Codes with Class-weight Consideration, *Information Sciences EIK* 16(5/6) (1979), 315-321.
12. Manohar Lal Kaushik; Necessary and Sufficient Number of Parity Checks in Codes correcting Random Errors and Bursts with Weight Constraints under a New Metric, *Information Sciences* 19 (1979), 81-90.
13. Manohar Lal Kaushik; Channels and Bounds for Class-Metric Codes, *Revue Roumaine de Mathematiques Pures et Appliqués TOME* XXVI, 10 (1981), 1345-1350.
14. W. C. Huffman, J-L Kim and P. Solé; *Concise Encyclopedia of Coding Theory*, CRC Press, 2021.
15. Michel Marie Deza, Elena Deza; *Encyclopedia of Distances* (Fourth Edition). Springer-Verlag, 2016.
16. A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé; The Z4-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory* 40 (1994) 301-319.
17. F. J. MacWilliams, N. J. A. Sloane and J.-M. Goethals; The MacWilliams Identities for Nonlinear Codes, *The Bell System Technical Journal*, 51(4) (1972), 803-821.